IBM BigFix Compliance

Compliance User's Guide

Version 9.2

IBM BigFix Compliance

Compliance User's Guide

Version 9.2

Note

Before using this information and the product it supports, read the information in "Notices" on page 49.

This edition applies to version 9, release 2, modification level 0 of IBM Endpoint Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

BigFix Compliance is a component of IBM BigFix Compliance, which includes vulnerability detection libraries and technical controls and tools that are based on industry practices and standards for endpoint and server security configuration (SCM checklists). The vulnerability detection libraries and the technical controls enable continuous, automated detection and remediation of security configuration issues.

BigFix Compliance provides report views and tools for managing the vulnerability of Security Configuration Management checks.

BigFix Compliance generates the following reports, which can be filtered, sorted, grouped, customized, or exported with the use of any set of BigFix Compliance properties:

- Overviews of Compliance Status, Vulnerabilities, and History
- Checklists: Compliance Status and History
- Checks: Compliance Status, Values, and History
- Vulnerabilities: Rollup Status and History
- Vulnerability Results: Detailed Status
- Computers: Compliance Status, Values, Vulnerabilities, and History
- Computer Groups: Compliance Status, Vulnerabilities, and History
- Exceptions: Management, Status, and History

New features

The following features and enhancements are included in BigFix Compliance BigFix Compliance 1.7.

- Single Sign-On user authentication using SAML 2.0
- Single Sign-On user authentication using LTPA Token
- Added REST API Token revocation
- Update to IBM Java 8.0.1.10
- Update to WebSphere Application server 8.5.5.7 Liberty Profile

System Requirements

Set up your deployment according to the system requirements to successfully deploy BigFix Compliance.

Configure your BigFix Compliance deployment according to the following requirements:

Table 1. Supported components and system requirements to deploy BigFix Compliance

Components	**Requirements**
Supported browser versions	• Internet Explorer versions 10.0, 11.0 • Firefox 31 and later versions • Firefox Extended Support Release (ESR) versions 31 and 38 • Google Chrome 35.0 and later versions
Supported IBM BigFix component versions	• Console versions 9.0, 9.1, 9.2 • Web Reports versions 9.0, 9.1, 9.2 • Windows Client versions 9.0, 9.1, 9.2 • UNIX Client versions 9.0, 9.1, 9.2
BigFix Compliance server operating system requirements	• Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows 2012 R2 **Note:** BigFix Compliance supports operating systems with the 64-bit versions only.
BigFix Compliance database server requirements	• Microsoft SQL Server 2008 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 **Note:** BigFix Compliance supports servers with the 64-bit versions only.
BigFix Compliance server	You must have Administrator privileges on the target BigFix Compliance server.
BigFix Compliance database	You must have dbcreator permissions on the target BigFix Compliance database server.
IBM BigFix database user permissions	IBM BigFix database user permissions
SCM mastheads and Fixlet sites	• You might have earlier BigFix Fixlets and custom Fixlets for security compliance in your deployment. These Fixlets continue to function correctly, but only certain Fixlets display within the BigFix Compliance reports. • To view the current list of SCM content sites that are supported with BigFix Compliance, see the technote **What SCM content is available for TEM?**.
IBM BigFix DB2 database permissions	You must have data administration authority (DATAACCESS) to perform the following tasks: • Access to create objects • Access to data within a IBM BigFix DB2 database

Note: Version 1.5.78 is the minimum version required to upgrade to Compliance 1.7.30.

General Usage Concepts

Navigation

Using BigFix Compliance, you can navigate and explore security configuration check results. Each computer in your deployment evaluates the appropriate Security Configuration Management checks that you have activated using the IBM BigFix console, and each computer reports a *pass*, *fail*, or *not applicable* status for each check. Each computer also reports computer properties and analysis values, such as Security Configuration Management check measured values that are active in your deployment.

SCM check results are aggregated by the BigFix Compliance server and augmented by computer properties and analysis values to provide compliance overviews and detailed lists of results.

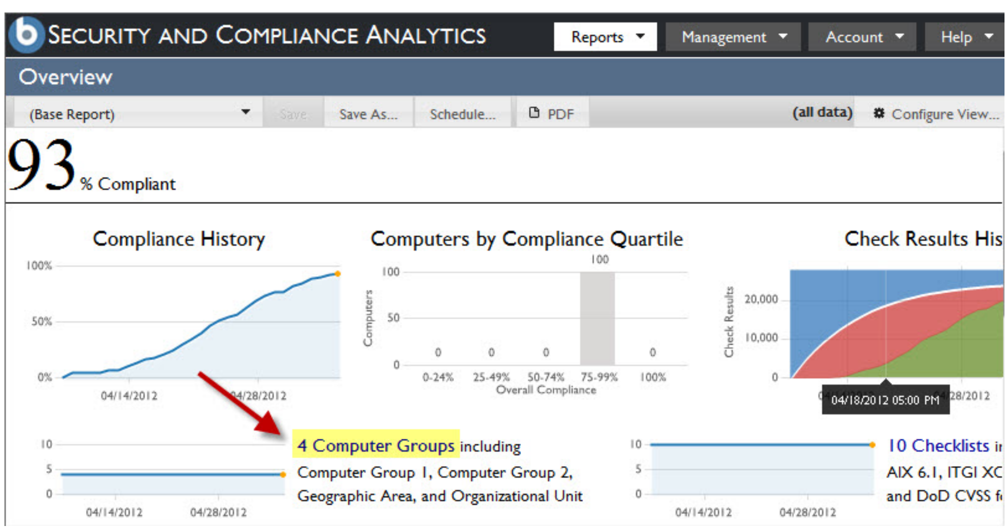
There are four primary navigation mechanisms in BigFix Compliance:
- Global navigation
- Linked navigation
- Sub-navigation (or scoped navigation)
- Saved Reports navigation

Global Navigation

Global Navigation refers to the primary drop-down menus at the top of the BigFix Compliance primary dashboard. Click the *Reports* drop-down menu to navigate through the different report types. Users with appropriate permissions also see a *Management* drop-down menu to view and manage the deployment configuration.

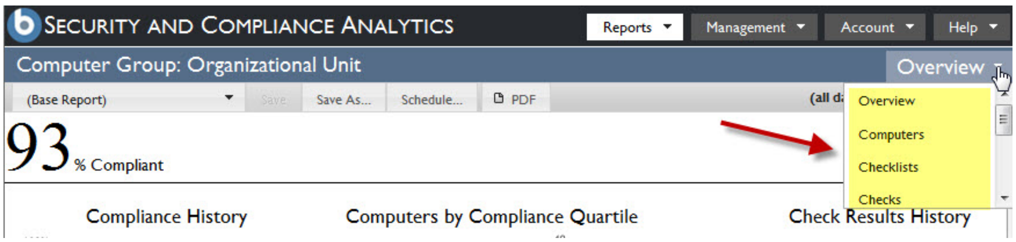
Linked Navigation

You can use linked text to navigate through report types. For example, click *5 Computer Groups* on the Overview report to display the related Computer Groups report.



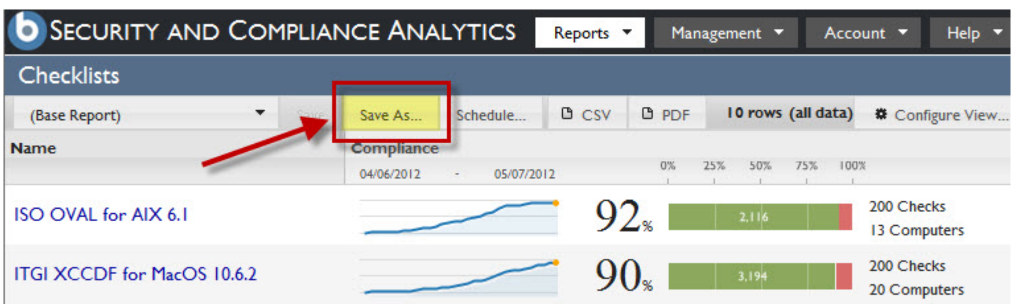
Sub-navigation

You can also explore reports within a given scope from the sub-navigation menu. To view all checks, all computers, or all exceptions appropriate for a given checklist, click the *Overview*drop-down menu that is located on the upper-right side of any overview report. The *List View* of reports will not show the *Overview* dropdown.



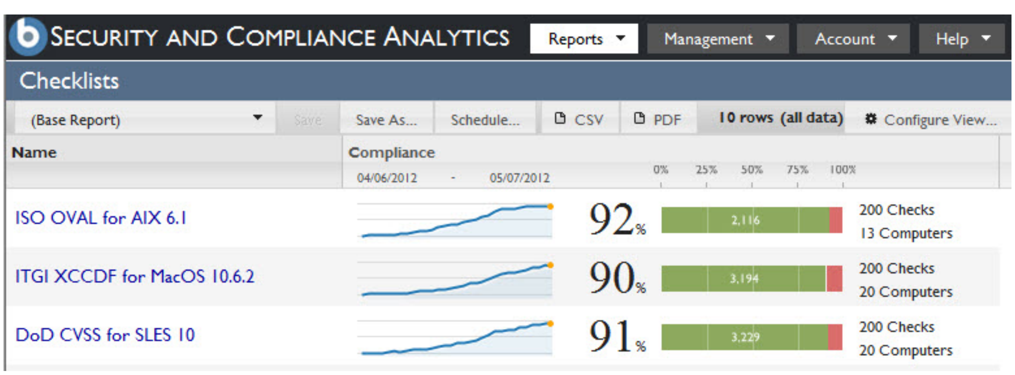
Saved Reports navigation

When you save a report view, it is available as a link on the Saved Reports list as well as from the Saved Reports menu on the left side of the report. Selecting a saved report from the menu regenerates the report view using the settings originally saved with the report. Click *Saved Reports* from the Reports dropdown menu, or click *Save As* from within any report to save the current view preferences.



Graphical Report View

You can view a variety of graphical charts that display different aspects of the security data in your deployment. You can select the columns to be displayed, change column arrangement, and filter data.



Configuring a report resource as the default view

Set default views for report resources to reduce steps that are needed to access reports when you are loading resources.

About this task

Use the Set as default option to configure a specific report as the default view when you are loading any report. The option reduces the steps that are needed to access reports when you are loading resources, including the following resources.

- Overview
- Detailed report views
- Grid report views for checklists, vulnerabilities, exceptions, computers, and computer groups

Users can set the default view based on their credentials:

- Standard users can configure reports to have private or default view settings.
- Administrators can configure reports to have private, default, or global default view settings.

You can set a report to have the following settings:

Private
: This option makes the report private.

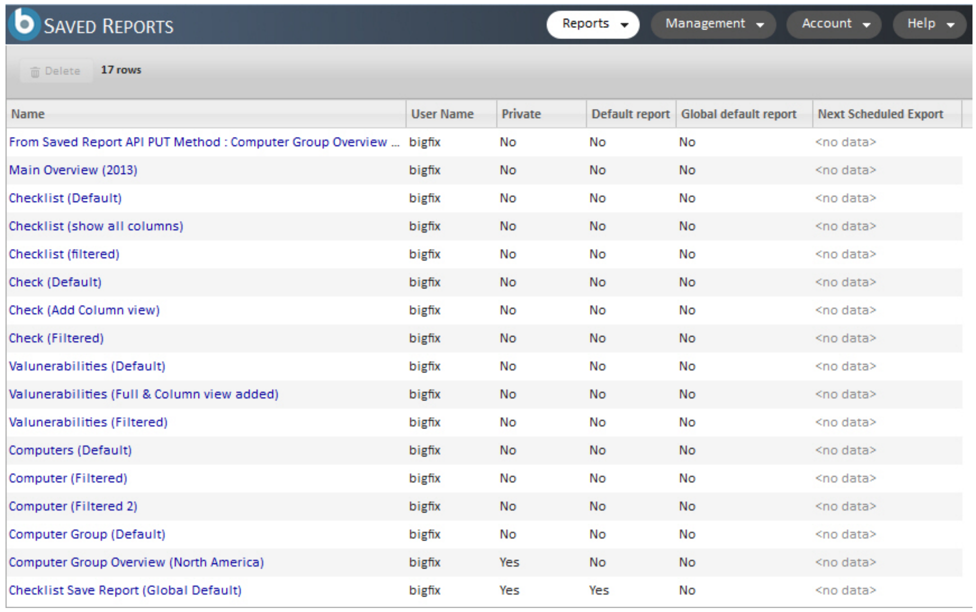
Set as default
: This option saves the report as the default view for the user of that specific report page.

Set as global default
: This option saves the report as the global view for all users of that specific report who do not have it set as their default report page.

  Only administrators can save reports to have a global default view. However, when a standard user already set a report as the default, the administrator cannot overwrite that default report view.

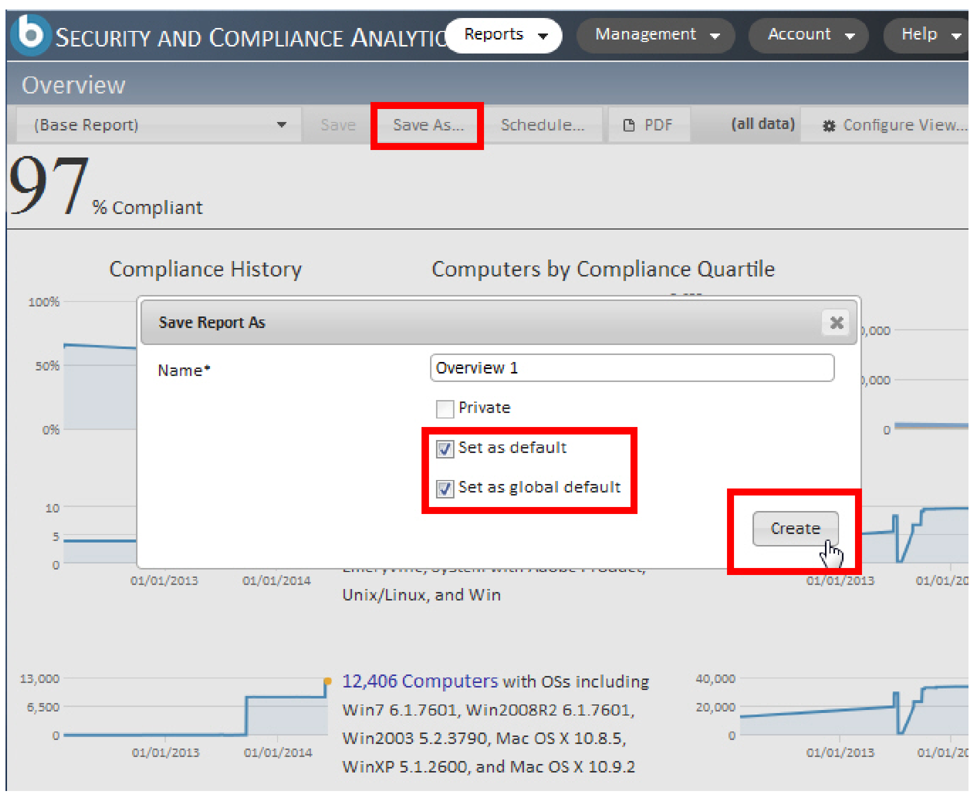
Procedure

1. Go to **Reports** > **Saved Reports** and select the report that is to be saved as the default report view.

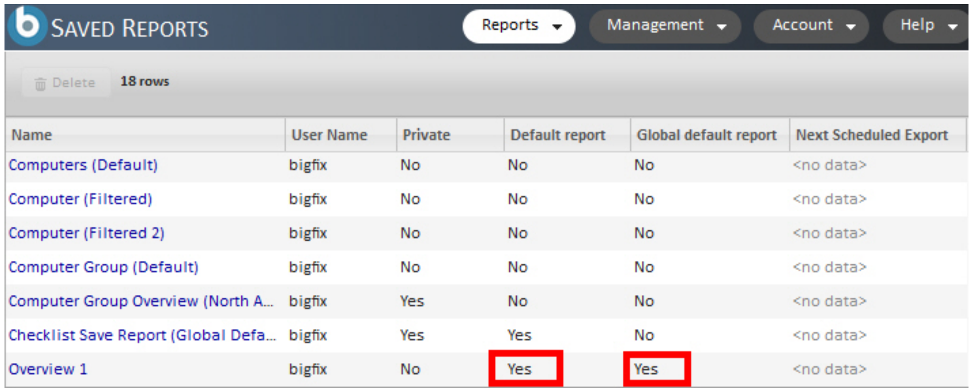


Name	User Name	Private	Default report	Global default report	Next Scheduled Export
From Saved Report API PUT Method : Computer Group Overview ...	bigfix	No	No	No	<no data>
Main Overview (2013)	bigfix	No	No	No	<no data>
Checklist (Default)	bigfix	No	No	No	<no data>
Checklist (show all columns)	bigfix	No	No	No	<no data>
Checklist (filtered)	bigfix	No	No	No	<no data>
Check (Default)	bigfix	No	No	No	<no data>
Check (Add Column view)	bigfix	No	No	No	<no data>
Check (Filtered)	bigfix	No	No	No	<no data>
Valunerabilities (Default)	bigfix	No	No	No	<no data>
Valunerabilities (Full & Column view added)	bigfix	No	No	No	<no data>
Valunerabilities (Filtered)	bigfix	No	No	No	<no data>
Computers (Default)	bigfix	No	No	No	<no data>
Computer (Filtered)	bigfix	No	No	No	<no data>
Computer (Filtered 2)	bigfix	No	No	No	<no data>
Computer Group (Default)	bigfix	No	No	No	<no data>
Computer Group Overview (North America)	bigfix	Yes	No	No	<no data>
Checklist Save Report (Global Default)	bigfix	Yes	Yes	No	<no data>

2. From the **Edit Report** panel, configure the report to be viewed with any of the following options.
   - Private
   - Set as default
   - Set as global default



3. Click **Create**.

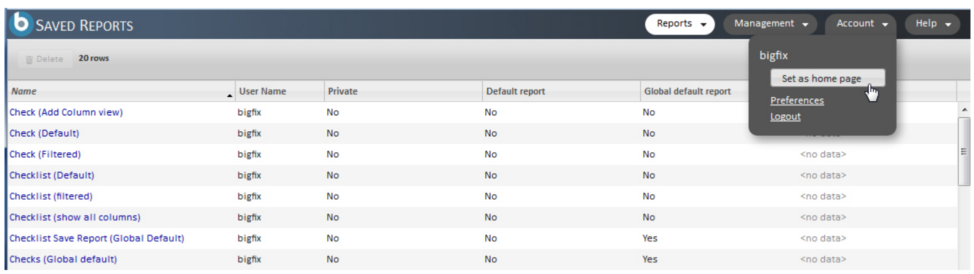


Configuring a report resource as the home page

Set any page or report resource, including saved reports, as the home page.

Procedure

1. Go to the page you want to set as the home page.
2. From the upper right corner, select the **Account** menu and click **Set as home page**. When a page is currently set as the home page, the option is disabled.



Results

Your next log in will open to the page you selected.

Using the autosize columns feature

Columns in BigFix Compliance reports are set by default to automatically resize to fit a grid window.

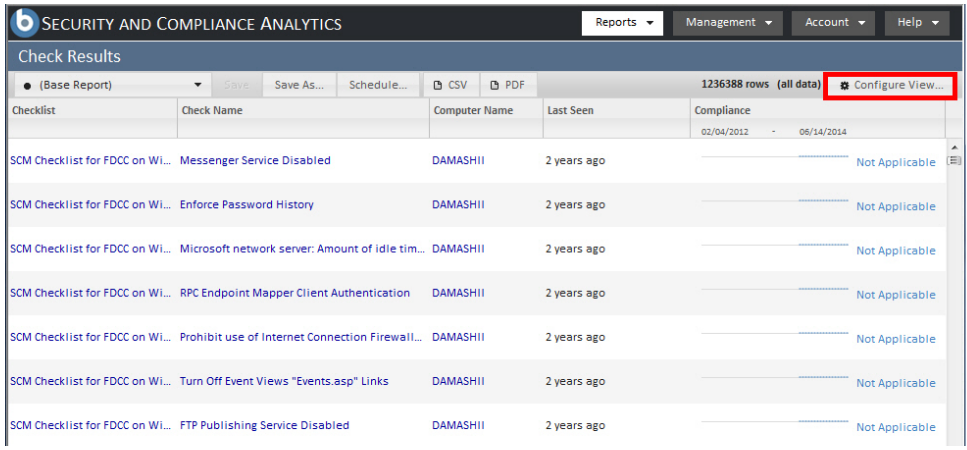
About this task

When the report you are using has several columns, you can use the Autosize Columns feature to view several columns without compressing the column views. You can also scroll horizontally across the visible report grid window. You can also set the autosize feature when you are creating a saved report. Creating a saved report with Autosize Columns disabled will retain all column widths even if the column widths exceed or are less than the visible grid area.

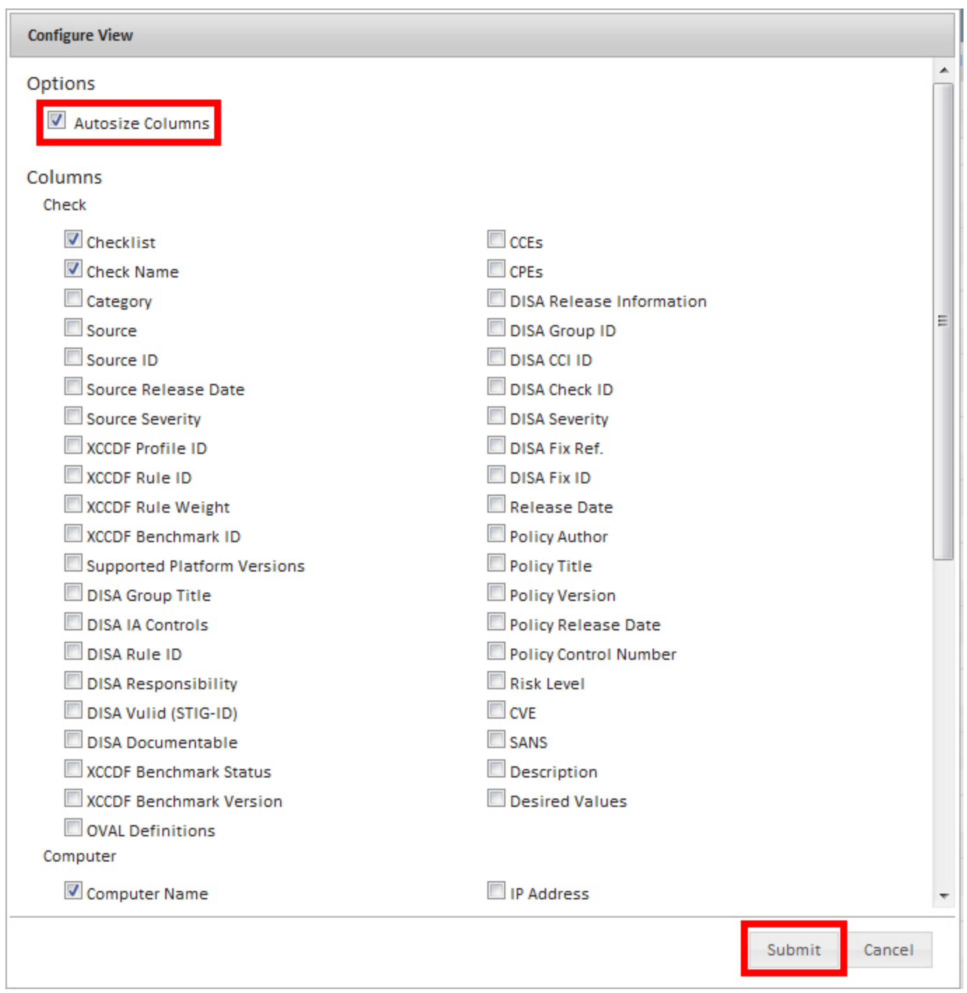
This feature is enabled by default.

Procedure

1. From an open report that uses columns, click **Configure View...**.



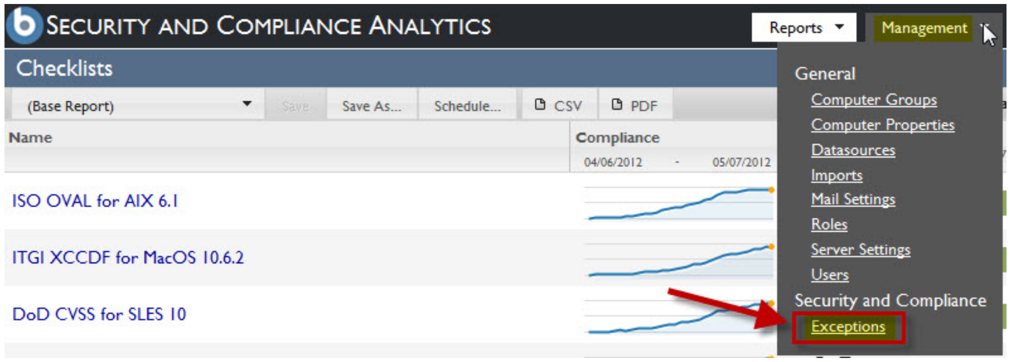
2. From the **Configure View** windows, you can either select or clear the **Autosize Columns** checkbox.



3. Click **Submit**.

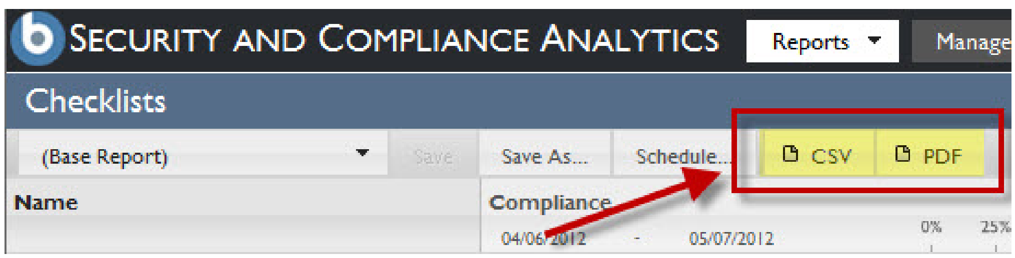
Managing exceptions

You can set exceptions to exclude data from your compliance reports. From the Management drop-down menu, click *Exceptions*.



Exporting

You can export the data view of most report views to a .CSV or .PDF formatted file on your local computer. Click the *.CSV* or *.PDF* links on the top bar of the console.



Chapter 2. Viewing deployment compliance status reports

You can view the compliance status in your deployment from any of the four report types.

BigFix Compliance reports display graphical and tabular views of different aspects of your deployment compliance status.

There are four main report types available, each of which displays a different, configurable view of the current and historical compliance status of the deployment. All users with accounts on the system can see all report types, but the data visible to each user depends on the computers to which they have been granted visibility.

For a graphical representation of each report type, see Example Reports in the Appendix.

Overview Reports

The following graphical reports are available from the primary Overview window in the SCA dashboard:

Deployment Overview
: Shows deployment information (such as quantity of computers and quantity of checks) and overall, historical aggregate compliance for all checks on all computers visible to logged-in users.

Checklist Overview
: Shows information about a single checklist (such as quantity of checks in the checklist) and overall, historical aggregate compliance for the checklist as applied to all computers visible to logged in users.

Computer Overview
: Shows information about a single computer (such as number of checks evaluated on the computer) and overall, historical aggregate compliance of all checks evaluated by the computer.

Computer Group Overview
: Shows information about a computer group (such as number of children/sub-groups and number of member computers) and overall, historical aggregate compliance of the group.

Check Overview
: Shows information about a single check (such as check source and check description) and overall, historical aggregate compliance of the check as evaluated by all computers visible to logged in users.

Vulnerability Overview
: Shows information about a single vulnerability check (such as vulnerability properties, CVSS score metrics, and vulnerability description) and overall, historical aggregate compliance for the vulnerability evaluated by all computers visible to logged in users.

List Reports

Click **Reports** to find the following reports:

Checklist List
Shows the list of checklists in the deployment together with attributes of each checklist and the overall, historical aggregate compliance results of all checks on all visible computers for each checklist.

Checks List
Shows the list of checks in the given scope together with attributes of each check and the overall, historical aggregate compliance results (the aggregate of all visible computer's pass and fail score) of each check.

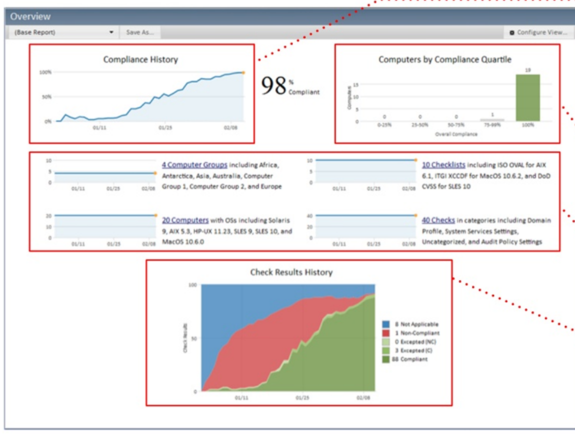
Computers List
Shows the list of all computers in the given scope visible to the logged-in user together with attributes of each computer and the overall, historical aggregate compliance results of all checks evaluated on the computer.

Computer Groups List
Shows the list of all computer groups in the given scope visible to the logged-in user together with attributes of each group and the overall, historical aggregate compliance results of all checks on all computers in each group.

Vulnerabilities List
Shows the list of vulnerability checks in the given scope visible to the logged-in user together with attributes of each computer and the overall, historical aggregate vulnerability results of all vulnerability checks evaluated on the computer.

The following annotated screen captures provide a summary of the functions of each report type.

Overview Reports



Compliance History: represents aggregate check results (pass/fail) across all computers within current scope. Excepted computers are counted as passing.

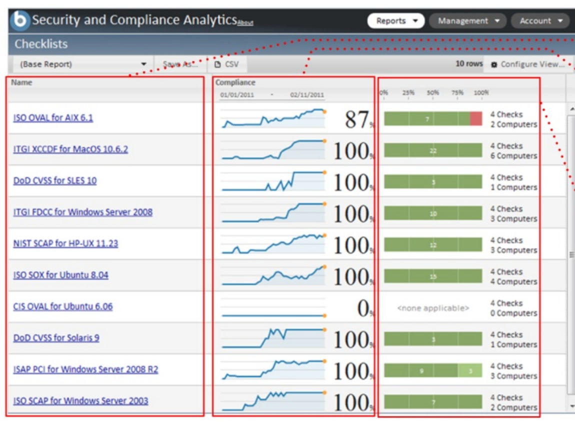
Computers by Compliance Quartile: represents computers grouped by computer compliance.

Deployment information: represents quantities of key components in the system.

Check Results History: represents aggregate check results (pass/fail) across all computers within current scope, grouped by check result status.

Overview Report types: Deployment Overview, Checklist Overview, Computer Overview, Computer Group Overview, Check Overview

List Reports



Name: lists each item represented for the list type.

Compliance: represents history of aggregate results (pass/fail) across all computers within current scope. Excepted computers are counted as passing.

Results: represents aggregate check results (pass/fail) across all appropriate computers within current scope, grouped by check result status.

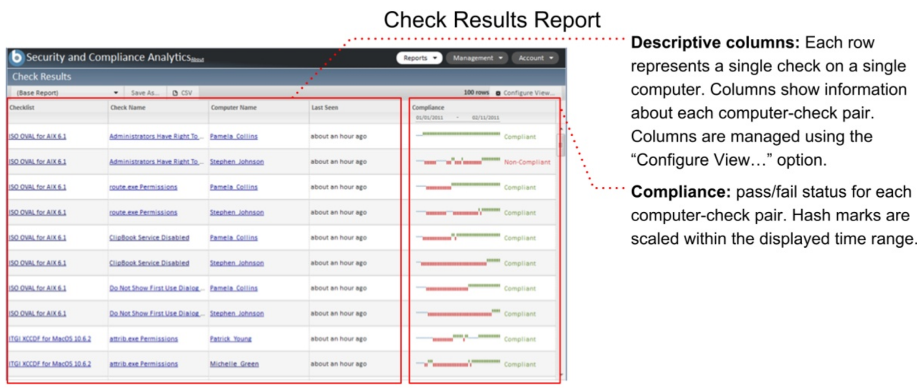
List Report types: Checklists list, Checks list, Computers list, Computer Groups list

Check Results Reports

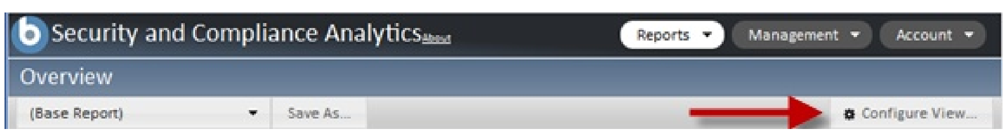
This report shows the list of all checks and computers, attributes of each computer and check, and the historical compliance result for each check on each computer.

Exceptions Reports

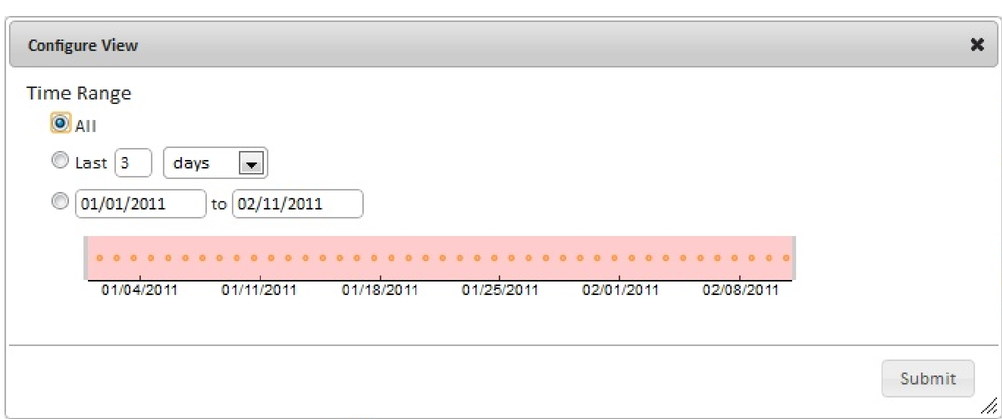
The Exceptions Report shows the list and status of exceptions in the given scope applied to each computer visible to the logged-in user, together with attributes of each check, each computer, and each exception.



To customize the settings of each report, such as filtering the view or adding additional columns, click *Configure View* to create custom settings.



You can set parameters for how your data is displayed in reports in *Configure View*.



Saved Reports

The Saved Reports feature retains a specific report format (including the displayed columns and filters you used to customize the view) for future use, without creating the same settings each time. When you save a report, it becomes available in the Saved Reports list report and visible in the drop-down box on the left side of the sub-navigation area when viewing that report type.

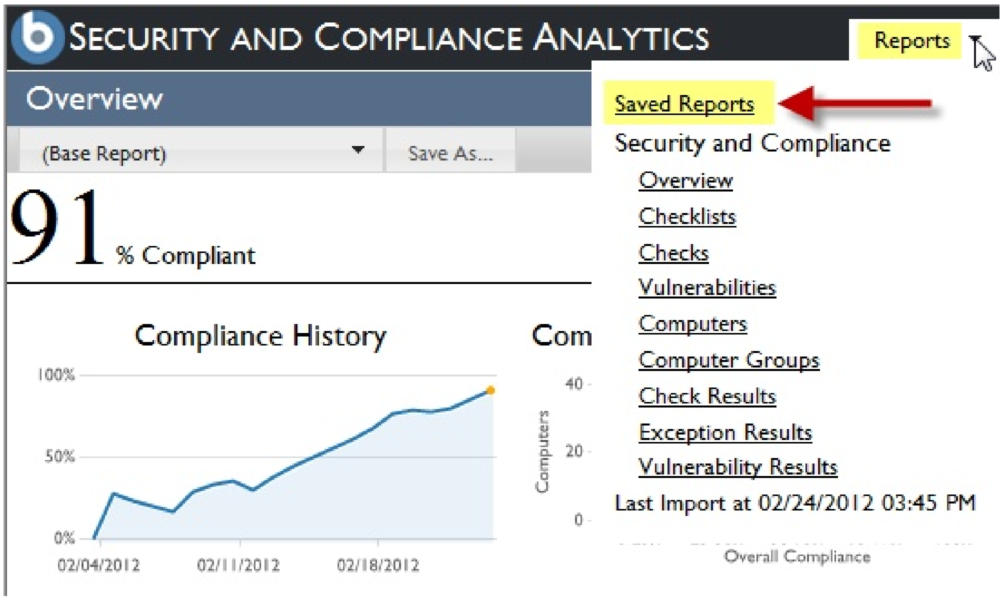


Chart Types

BigFix Compliance displays summaries of compliance data through the following chart types:

Compliance Overview
: Displays compliance history over time as an overall percentage.

Computers by Compliance Quartile
: Bar chart that provides compliance data by quartile.

Compliance History Detail Chart
: Win loss chart that displays compliance history over time.

Check Results History
: Total number of check results over time.

Not applicable
: A check that does not apply to a given computer.

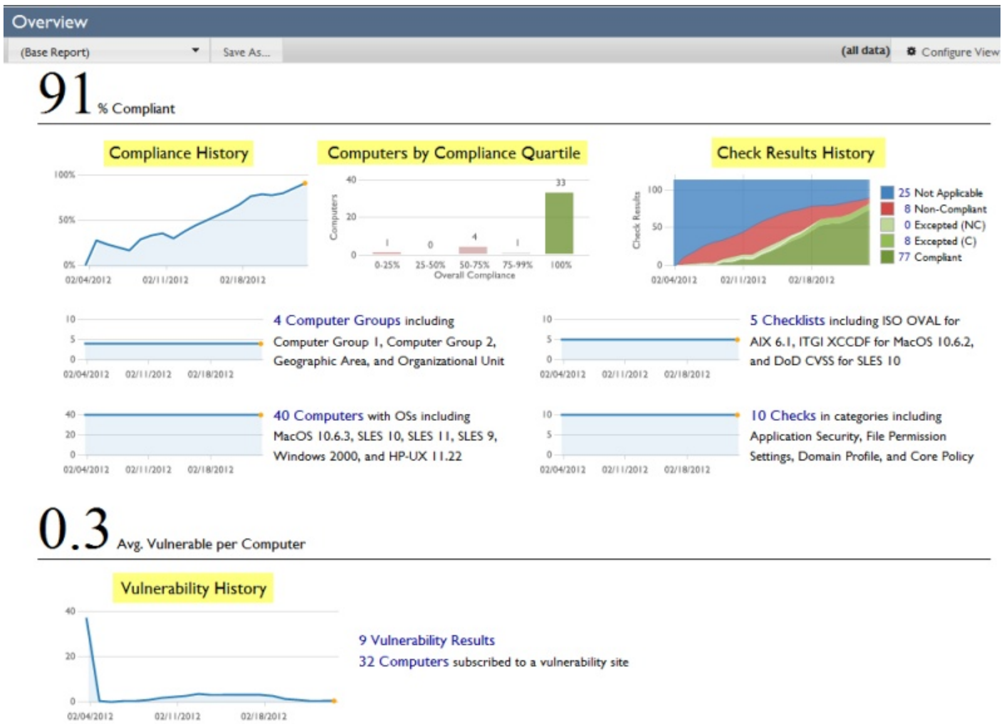
Noncompliant
: A check that is noncompliant on a given computer.

Excepted – (NC)
: A check that is noncompliant on a given computer, but that has been excepted through a manually-created exception.

Excepted – (C)
: A check that is compliant on a given computer, but that has been excepted through a manually-created exception.

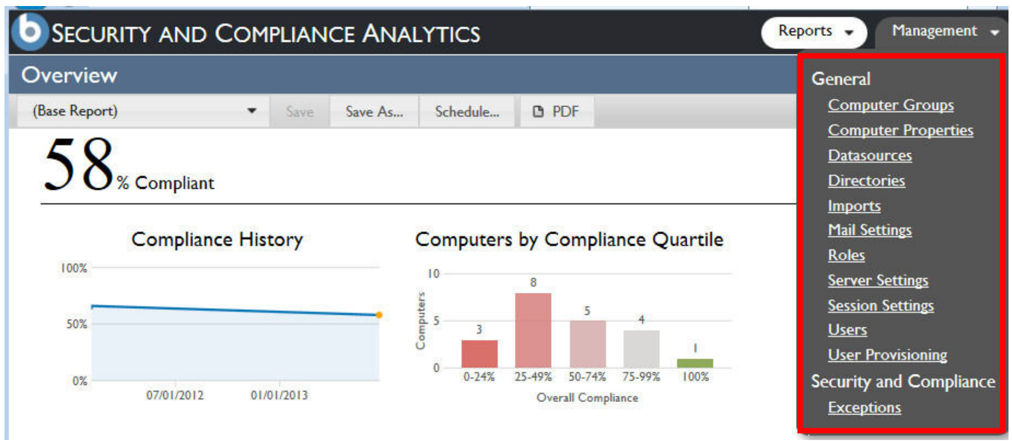
Compliant
A check that complies with the checklist desired values.

Vulnerability History Detail Chart
Win loss chart that displays vulnerability history over time.



Chapter 3. Management Tasks

The Management Tasks function within BigFix Compliance gives you control over various aspects of your compliance deployment. From the Management drop-down list, users with appropriate permissions can manage computer groups, computer properties, datasources, directories, imports, mail settings, roles, server settings, session settings, users, user provisioning, and exceptions.



Click **Management** to select any of the following tasks

- General
  - Computer Groups
  - Computer Properties
  - Datasources
  - Directories
  - Imports
  - Mail Settings
  - Roles
  - Server Settings
  - Session Settings
  - Single Sign-on Settings
  - Users
  - User Provisioning
- Compliance
  - Exceptions

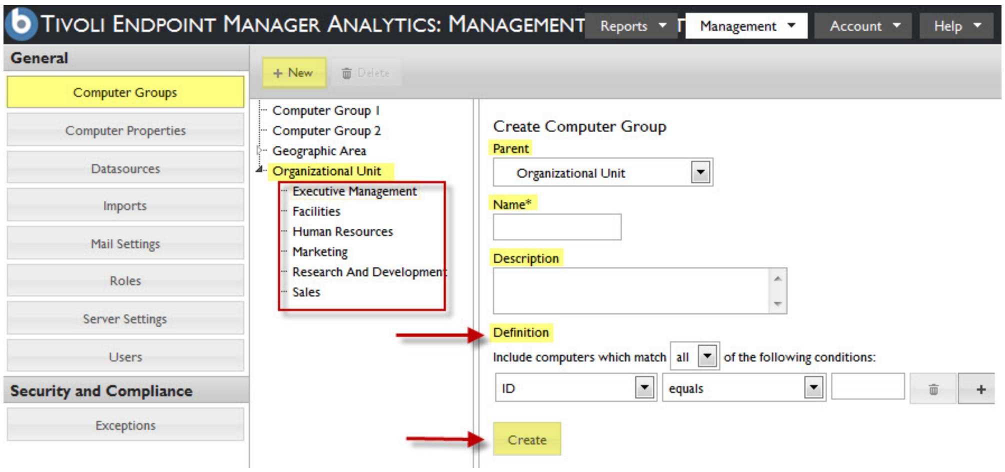
Computer Groups

BigFix Compliance computer groups help you organize the compliance data that displays in your reports. Specifically, you can filter data to limit what you want to see displayed in your overviews and lists.

All users need to be assigned to a computer group in order to log in to BigFix Compliance. Logged-in users can see compliance data based on their associated computer group.

To create a computer group, click the **Management** drop-down menu at the top of the console and select **Computer Groups**. Click **New**. Use the dropdown menu to assign your group to a parent. Use the **Definition** field to assign parameters to your group.

When finished, click *Create*.

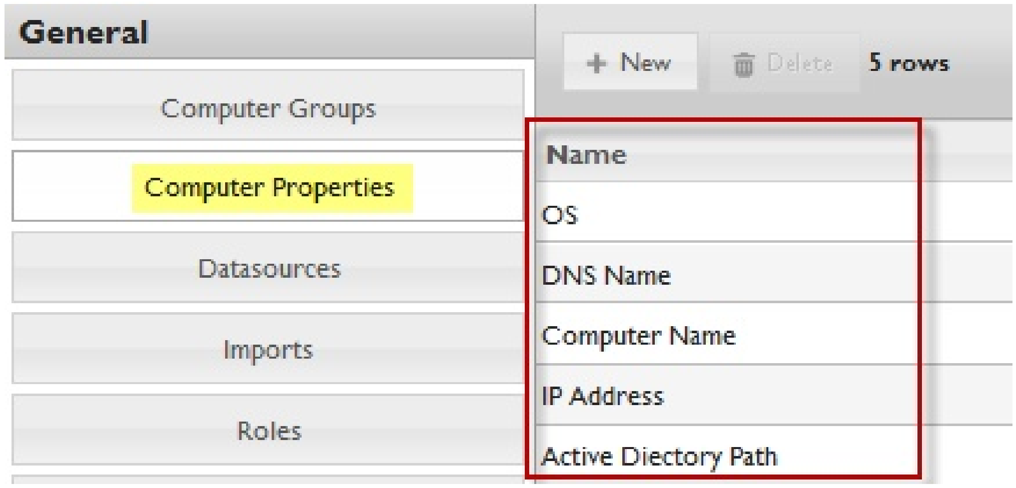


Note: You must perform an import after saving your changes.

You can set the Users account to configure multiple computer groups. To configure multiple groups, see "Configuring multiple computer groups" on page 25.

Computer Properties

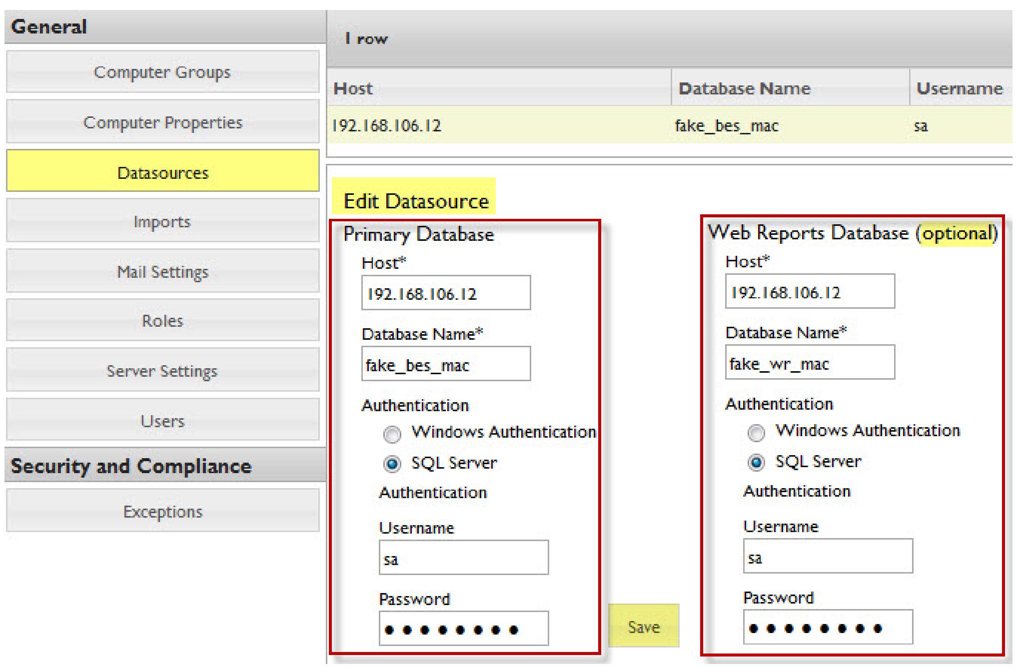
You can create computer properties from the BigFix Compliance datasources available for reporting and filtering within the Compliance interface. You can use the default properties in your console, or click *New* to create new properties. These computer properties become the display columns in the computers and results list view for your reports.



Note: You must perform an import after saving your changes.

Data Sources

Using datasources, you can view information about the IBM BigFix Compliance database from which your BigFix Compliance compliance data is based. You can also view information about the Web Reports database that is the source of some or all of your BigFix Compliance users. The Web Reports connection provides a single-sign-on capability for users between Web Reports and BigFix Compliance. You cannot edit these settings after the initial setup but you can add the Web Reports database information if you originally skipped this step.



Adding a data source

Add a data source to view information about the database on which your compliance data is based.

Before you begin

When you are adding a data source:

- Do not add a datasource that is a DSA copy of an existing datasource to avoid the display of duplicate data.
- If you restrict user access based on computer groups, you might have to create new computer groups or modify existing ones to ensure correct access restrictions for the new datasource.
- If you added new computer properties, ensure that you provide mappings to those properties in the new datasource.
- In BigFix Compliance, if you have exceptions that are based on computer groups, ensure that those exceptions and groups are set up correctly for the new datasource.
- In Software Usage Analysis (SUA), if you have contracts that are based on computer groups, ensure that those contracts and groups are set up correctly for the new datasource.
- You must run an import after you add a datasource before computers from that datasource are available in reports.
- When you are running an import, all datasources must be online and reachable or the import fails. This ensures that reports do not show incomplete data or misleading inventory or compliance aggregates.
- Regarding Report data, a user with restricted access by computer group sees only the results or computer report data for their assigned computer group. Examples of results or computer report data are Computers, Computer Groups, Check Results, Exception Results, and Vulnerability Results.

  All users still see all Checklists, Checks, and Vulnerabilities from all datasources, regardless of Computer Group restrictions. Multi-tenancy supports segmentation of computer data based on computer groups and a user's computer group membership. It does not support segmentation of checklists, checks, and venerability checks themselves or of a SUA software catalog.

  You must deploy multiple TEMA servers for the following cases:

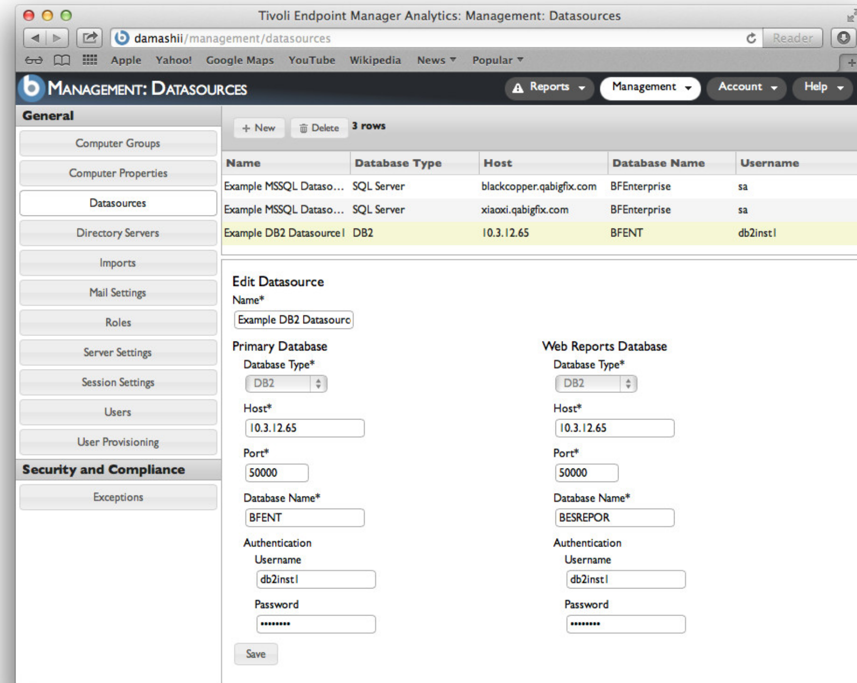
  - If you are not able to see the existence of checklists that are created for other customers
  - You have to apply different software catalogs for different customers,

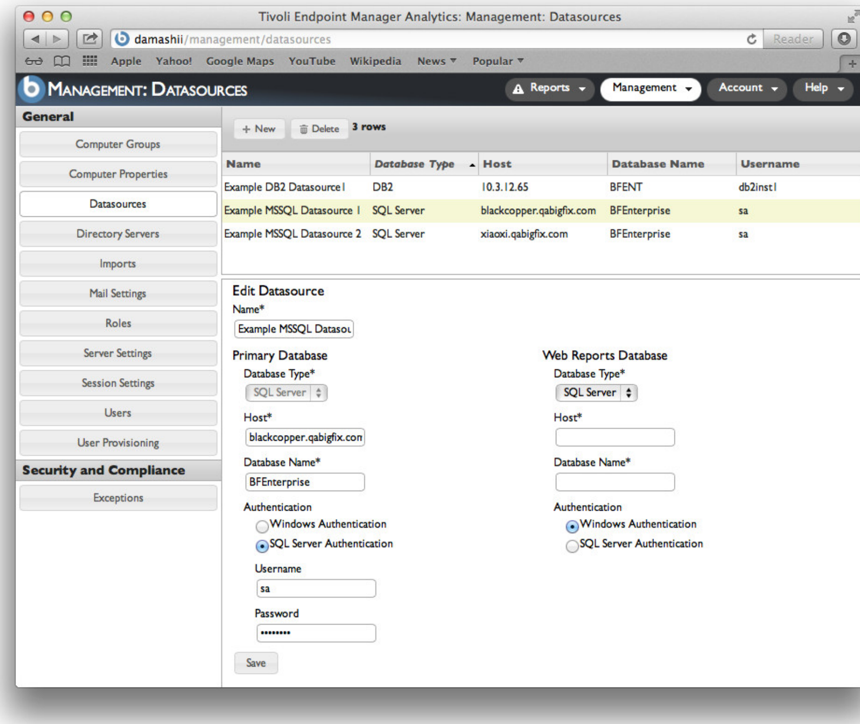
Procedure

1. In the upper right corner, click **Management** > **Data sources**.
2. In the upper left corner of the horizontal navigation bar, click **New**. A new form opens in the lower pane.
3. Provide the unique name for the new data source.
4. Select the database type from the **Database Type** drop-down list.

Option	Description
Database Type	**Steps**
DB2	1. Specify the host, port, and database name. 2. For server authentication, specify a user name and password.

Option	Description
SQL Server	1. Specify the host and database name. 2. Select the authentication type. 3. For SQL server authentication, specify a user name and password.





5. Click **Create**.

Deleting a data source

Procedure

1. In the upper right corner, click **Management** > **Data sources**.
2. In the upper pane, click the data source that you want to delete
3. In the upper left corner of the navigation bar, click **Delete**.

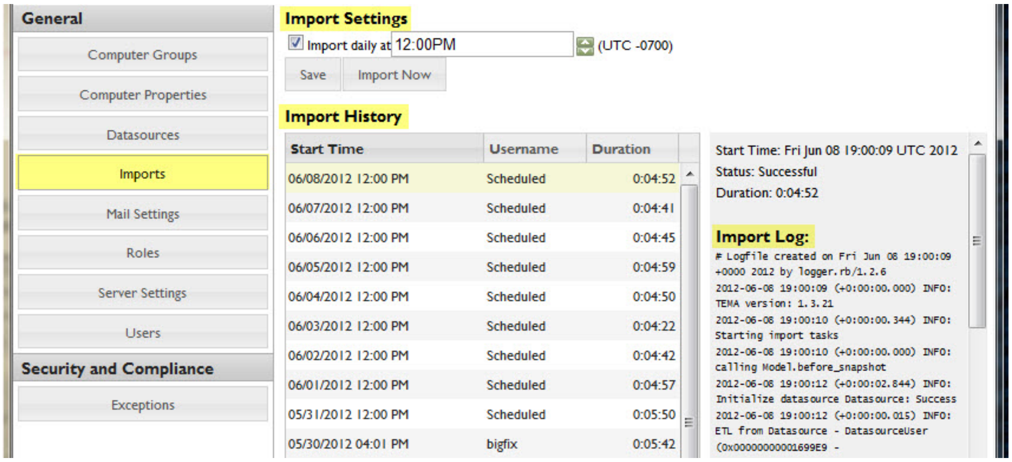
Results

You deleted all the data for computers that belong to this data source.

Imports

Use the Imports interface to schedule a recurring import, disable recurring imports, start a manual import, view current import status, and view logs of previous imports.

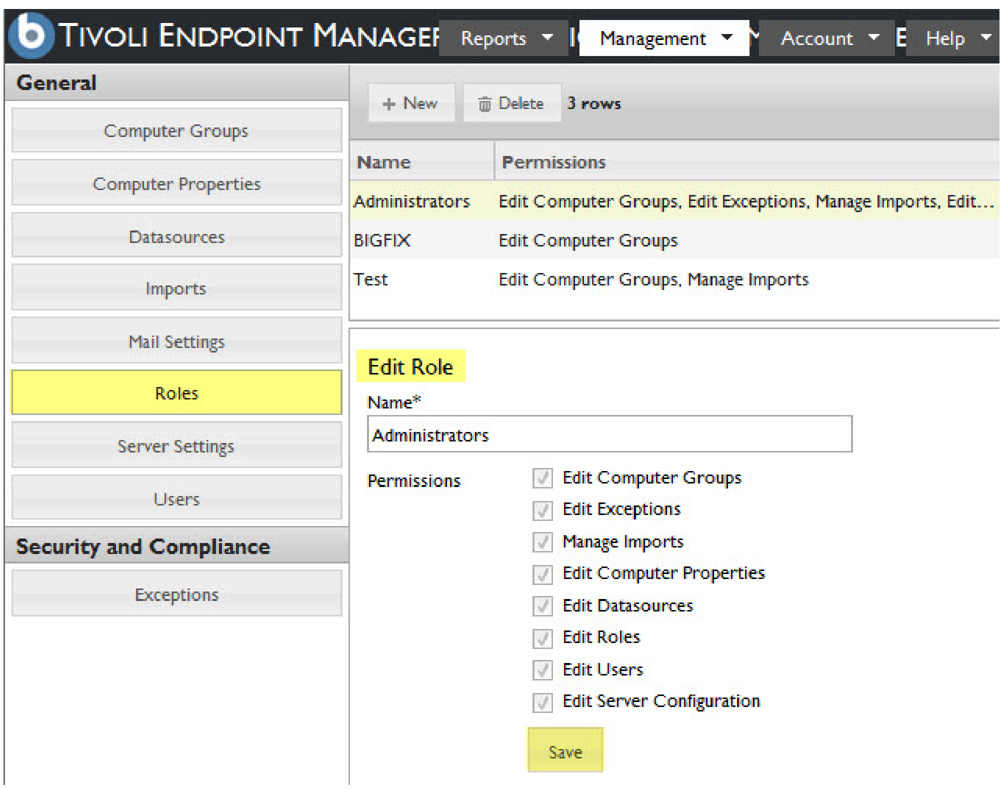
Run an immediate import by clicking *Import Now*. To schedule a recurring import, first check the import box at the top of the window and set the desired daily start time. Then click Save to confirm the change.



Roles

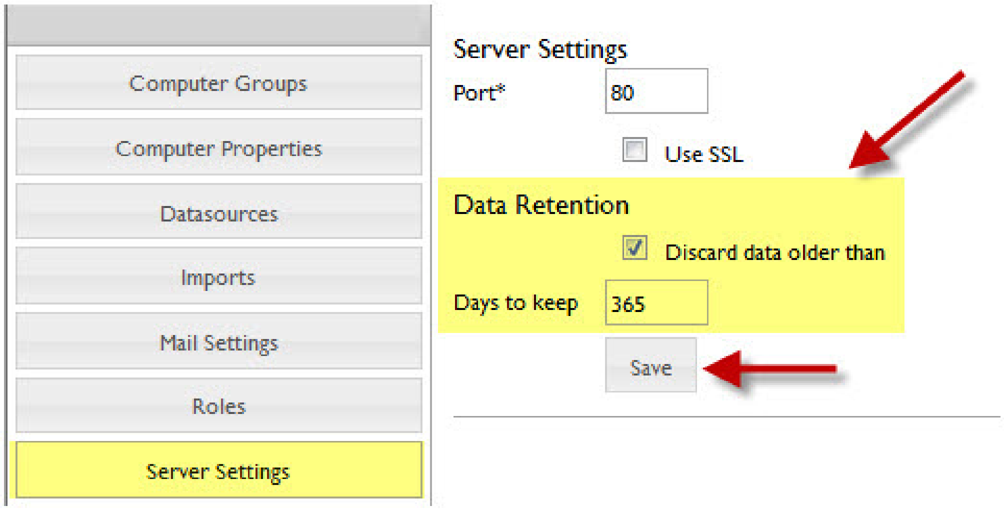
Use the Roles interface to assign new roles to users or edit existing roles. In this version of BigFix Compliance, the assignable permissions include Edit Computer Groups, Edit Exceptions, and Run Imports.

Use the buttons on the top bar to create new roles or delete existing roles.



Server Settings

Use the Server Settings interface to configure the HTTP port, SSL, and enable or disable data retention. Any changes to the port or SSL settings require a service restart.



Session Settings

You can change your session settings to specify the session time for a logged in user who is inactive for a certain period and to custom the message on the login page using Markdown text. The default session time out is set to 1 hour. To make changes in your session setting, go to **Management** > **Session Settings**. Make your changes to the session time out and the message then click **Save**.

Single Sign-on Settings

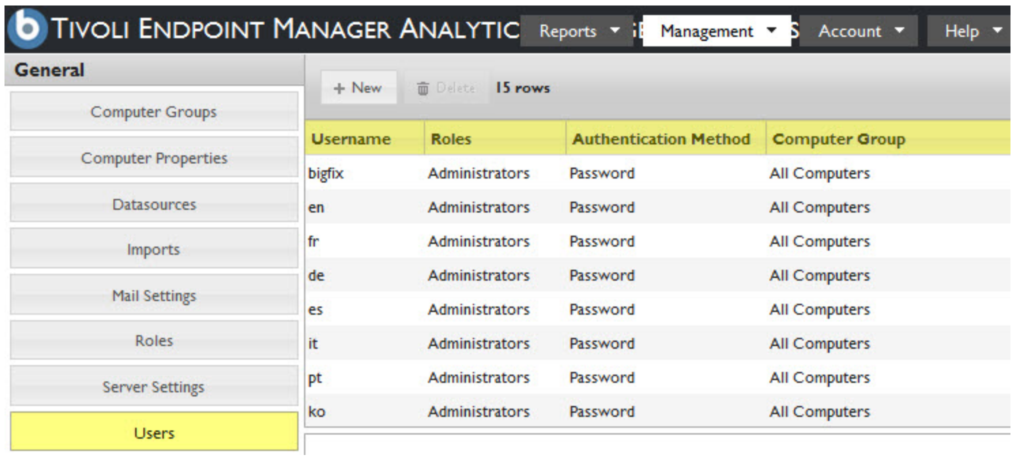
Configure your single sign-on settings in this section.

You can set your user authentication settings for the Security Assertion Markup Language Single Sign-on (SAML SSO) and Lightweight Third Party Authentication (LTPA).

For more information about configuring SAML SSO and LTPA authentication, see the BigFix Compliance Setup Guide.

Users

From the Users interface, you can create and edit users, assign roles, and assign a set of computer groups to which a user has access. Administrators can edit user passwords, email addresses, and contact information.



Configuring multiple computer groups

Before you begin

You must have Administrator privileges or use the Manage Computers Group role to configure user accounts to include multiple computer groups.

About this task

This feature enables non-Administrator users to view ranges for computer group compliance data by granting the user access to multiple computer group during user creation or user account updates.

Procedure

1. Log in to BigFix Compliance as an Administrator or using the Manage Computer Groups role.
2. From the navigation menu, click **Management**. Select **User** from the dropdown menu.
3. From the **Managers: Users** window, create a new user.
   a. Enter the details for the following fields:
   b. From the Computer Groups drop-down menu, select the computer groups that the new user will be associated with.
   c. Enter then confirm a password.
   d. Enter the email address.
4. From the top navigation menu, click **Reports**. Click **Import Now**.

What to do next

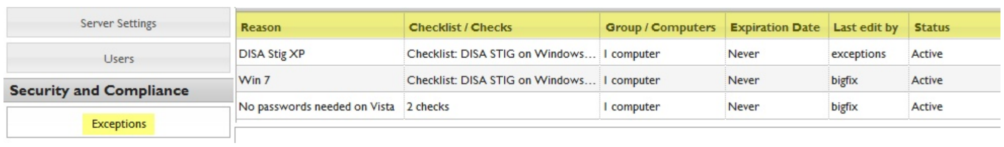
To confirm if the multiple group was configured correctly, login to the new user account that has more than one computer group associated with it.

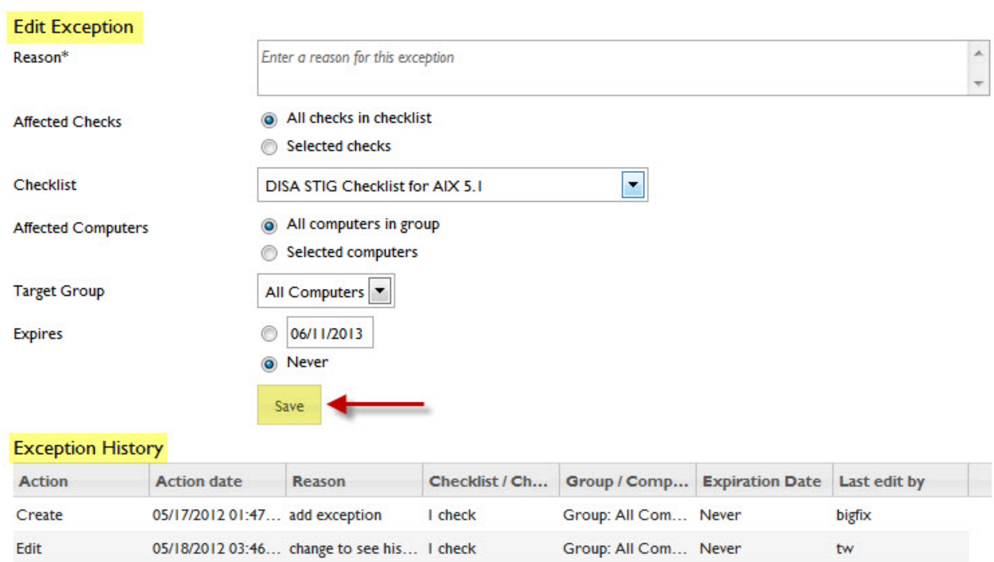
User Provisioning

Use the User provisioning feature to authenticate users within LDAP groups without creating users individually. See the BigFix Compliance Setup Guide to learn more about user provisioning and LDAP.

Exceptions

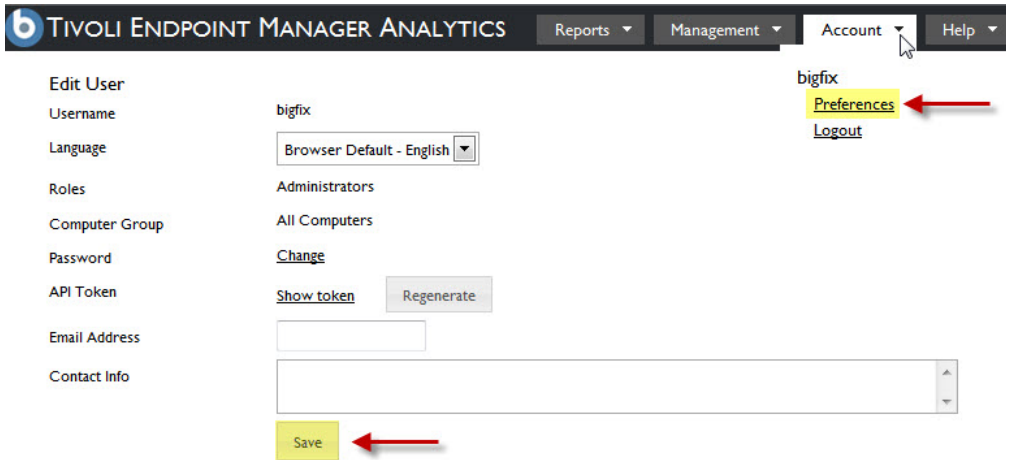
You can use the Exceptions menu to create and edit exceptions for checks, computers, computer groups, and checklists with or without an expiration date. You can also view a list of existing and active exceptions. To edit an exception, click an exception name in the list, and the Edit Exception and Exception History menus display.





Account Preferences

Use the Account Preferences interface to change passwords, contact information, or API tokens. Click the *Account* drop-down menu from the top of the window.



Chapter 4. Configuring report definitions using REST API

Administrators can use REST API to create, update, and delete saved report view definitions across BigFix Compliance instances.

Overview of REST API report definitions

The operations of the BigFix Compliance REST API protocol are defined as HTTP methods on certain REST resources.

Table 2. Target REST Operations

Target REST operation URI	HTTP methods	Purpose of the operation
`api/reports`	POST	Create a saved report item.
`api/reports`	PUT	Update a saved report item by ID.
`api/reports`	GET	Retrieve all saved report items.
`/api/reports/<id>`	GET	Retrieve a saved report item by ID.
`api/reports`	DELETE	Delete a saved report item by ID.

Path parameters

The `path` parameter specifies the report name that is used when configuring the report definitions.

Table 3. Path parameters of Security Compliance and Analytics reports

Report name	Path parameter
Overview	`/scm`
Checklists	`/scm/checklists`
Checks	`/scm/checks`
Vulnerabilities	`/scm/vulnerabilities`
Computers	`/scm/computers`
Computer Groups	`/scm/computer_groups`
Check results	`/scm/check_results`
Exception Results	`/scm/exception_results`
Vulnerability Results	`/scm/vulnerability_results`

Query parameters

Table 4. Query parameters

Parameter	Description
`token`	The API token for the target user.
`ID`	The saved report ID. This parameter is not used for input.

Table 4. Query parameters (continued)

Parameter	Description
user_id	The user ID of the report owner in TEMA. This parameter is not used for input.
pagestate_id	The page state ID that is specific to the report. This parameter is not used for input.
name	The name of the saved report.
path	The path that specifies the report (for example Overview, Computer Groups, and others).
private	The value is True for private and False for public.
state	
column	The columns in a saved report.
column_order	The order of the columns as specified by <column name" : <number>. The order of the column number starts from the left, with the smallest column number. The value of the number must be integers, such as 0, 1, 2, 3, and so on.
criteria	The conditions found in **Configure View** > **Filter**.
grid_options	The Autosize Columns options in **Configure View**.
autosize_columns	This parameter is present when Autosize Columns is on
order	
asc	The parameter that is true for ascending order; False for descending order
col	The parameter for the column to be sorted. The value is null for none.
time_range	
type	
all	The parameter for all types
relative	The parameter for the last *X* day/week/month/year
absolute	The parameter for a specific date range
units	"days", "weeks", "months", "years"
value	The value for the last X units
min	Starting datetime (range)
max	Ending datetime (range)
column_widths	The column widths that are specified by <column name> : <width>

Create a saved report

Use Rest API to create a saved report across BigFix Compliance instances.

Use the POST operation on the `api/reports` element to create a saved report.

Table 5. Operation details

Operation details	Description
Operation	`POST/api/reports`
Purpose	Create a saved report item.
HTTP method	`POST`
Request `content type`	`Application/json`
Normal HTTP response codes	`200 OK` + JSON data for single saved report definition that is created by POST

Error response codes

The following list includes the operation details for error response codes.

`500 + "Error: Name is already taken"`
When a duplicate post is made. The report is unique by name, user, and report category.

`500 + "Error: The property '#/' did not contain a required property of 'name' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}"`
When the header is missing `content-type: application/json`.

`401 Unauthorized + {"error":"There is no match for the provided user name and password"}`
When no token is provided.

`404 Not found`
When using unnecessary ID (`POST/api/reports/<id>`

`500 Internal Server Error ('Sorry something went wrong...')` + error in the TEMA log
When the JSON format is invalid.

`401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}`
When the token for the user has no computer assigned.

`404 + {"error":"Sequel::RecordNotFound"}`
When the ID is invalid.

`404 + {"error":"Sequel::RecordNotFound"}`
When accessing the private report of another user.

`500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}`
When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

`500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-`

a083dc10ee61#"}
: When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}
: When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Update a saved report

Use Rest API to update a saved report across BigFix Compliance instances.

Use the PUT operation on the `api/reports` element to update a saved report by ID.

Table 6. Operation details

Operation details	Description
Operation	`PUT/api/reports`
Purpose	Update a saved report item.
HTTP method	`PUT`
Request `content type`	`Application/json`
Normal HTTP response codes	`200 OK` + JSON data for single saved report definition that is updated by PUT

Error HTTP response codes

The following list includes the operation details for HTTP error response codes.

500 - "Error: The property '#/' did not contain a required property of 'name' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"
: When the header is missing `content-type: application/json`.

500 + {"Error":"the before_save hook failed"}
: PUT with non-owner's token.

401 Unauthorized + {"error":"There is no match for the provided user name and password"}
: When no token is provided.

404 Not Found
: When the ID is missing.

500 Internal Server Error ('Sorry something went wrong...') + error in the TEMA log
: When the JSON format is invalid.

401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}
: When the token for the user has no computer assigned.

404 + {"error":"Sequel::RecordNotFound"}
: When the ID (#) is invalid.

404 + {"error":"Sequel::RecordNotFound"}
When accessing the private report of another user.

500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}
When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-a083dc10ee61#"}
When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}
When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Retrieve all saved report items

Use Rest API to retrieve all saved report items across BigFix Compliances instances.

Use the GET operation on the `api/reports` element to create a saved report by the report ID.

Table 7. Operation details

Operation details	Description
Operation	`GET/api/reports/<report id>`
Purpose	Retrieves all saved report items.
HTTP method	`GET`
Request `content type`	`Application/json`
Normal HTTP response codes	`200 OK` + JSON data (total count + array of saved report definitions)

Error HTTP response codes

The following list includes the operation details for HTTP error response codes.

401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}
When the token for the user has no computer assigned.

401 Unauthorized + {"error":"There is no match for the provided user name and password"}
When no token is provided.

404 + {"error":"Sequel::RecordNotFound"}
When the ID (#) is invalid.

404 + {"error":"Sequel::RecordNotFound"}
When accessing the private report of another user.

500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}
When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-a083dc10ee61#"}
When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}
When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Retrieve saved reports by report ID

Use Rest API to retrieve a saved report by ID across BigFix Compliance instances.

Use the GET operation on the `api/reports` element to create a saved report by the report ID.

Table 8. Operation details

Operation details	Description
Operation	`GET/api/reports/<report id>`
Purpose	Retrieves all saved report items using the report ID.
HTTP method	`GET`
Request `content type`	`Application/json`
Normal HTTP response codes	`200 OK` + JSON data for single saved report definition that is specified by ID.

Error HTTP response codes

The following list includes the operation details for HTTP error response codes

401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}
When the token for the user has no computer assigned.

401 Unauthorized + {"error":"There is no match for the provided user name and password"}
When no token is provided.

404 + {"error":"Sequel::RecordNotFound"}
When the ID (#) is invalid.

404 + {"error":"Sequel::RecordNotFound"}
: When accessing the private report of another user.

500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}
: When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-a083dc10ee61#"}
: When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}
: When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Delete a saved report item by ID

Use Rest API to update a saved report item by ID across BigFix Compliance instances.

Use the DELETE operation on the `api/reports/<id>` element to Delete a saved report by id.

Table 9. Operation details

Operation details	Description
Operation	`DELETE/api/reports/<id>`
Purpose	Deletes a saved report item.
HTTP method	`DELETE`
Request `content type`	`Application/json`
Normal HTTP response codes	`204 No Content`

Error HTTP response codes

The following list includes the operation details for HTTP error response codes.

403 Forbidden + {"Error":"Access Blocked"}
: DELETE with the token of the non-owner, even if with administrative privilege.

404 Not Found
: When the ID is missing.

401 Unauthorized + {"error":"There is no match for the provided user name and password"}
: When no token is provided.

401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid

Computer Group. Contact your administrator for assistance."}
: When the token for the user has no computer assigned.

404 + {"error":"Sequel::RecordNotFound"}
: When the ID is invalid.

404 + {"error":"Sequel::RecordNotFound"}
: When accessing the private report of another user.

500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}
: When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-a083dc10ee61#"}
: When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}
: When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Chapter 5. Disaster Recovery for BigFix Compliance

Use the standard cold standby method of creating a backup and restoring the system in your disaster recovery plan for BigFix Compliance.

Similar to the IBM BigFix disaster plan, BigFix Compliance uses a standard backup/restore method that is called the Cold Standby method. This method does periodic backups of the application server and database files, usually done nightly. If there is a problem, the database and application server files can be restored to the IBM BigFix Application Server computer or another computer. The system is also restored.

Table 10. Pros and cons of using the cold standby method

Pros	Cons
• Simple and allows for multiple backups over time. • Does not require any additional hardware. Hot or cold standby computer is optional.	• All information since the last backup is lost in the event of a failure. • Restoring the system from the backup might have significant downtime.

The disaster recovery plan covers steps for the following procedures:
1. Backup procedure
2. Recovery procedure
3. Recovery verification procedure

Creating a backup of the application server

Create backups of the files and folders that the application server uses.

Establish a maintenance plan for nightly backups for the TEM_Analytics databases using SQL Server Enterprise Manager. Multiple backup copies give greater recovery flexibility. Consider backing up to a remote system to allow for higher fault tolerance.

For recovery purposes, create backups of the following files and folders that the application server uses:
- `[TEMA Application folder]\config` -- Configuration (HTTPS, Port number, database connection information, and others)
- `[TEMA Application folder]\log` -- Archived Import, error, and access logs

Recovering the backup application server

Restore the backup of your BigFix Compliance application server.

Procedure

1. Install the same version of SQL Server that was previously used in either a previous application server computer or a new computer.

   Note: If you used Mixed Mode Authentication on the previous application server, you must enable it for your new SQL installation.

2. Restore the TEM_Analytics databases from backup.
3. Install the application server. Use the same version of the application installation binary as was previously used.
4. At the end of installation, skip the launch web configuration step. Instead, go to NT Services Manager and stop 'Tivoli Endpoint Manager Analytics' service.
5. Restore/Replace the backed up configuration and log files and folders. Create the directory structure as needed.
6. Go to **NT Services Manager** and start the **Tivoli Endpoint Manager Analytics** service.

   Ensure that the new application server computer can access the following datasources: BFEnterprise and BESReporting. For NT Auth to access the TEM_Analytics and BFEnterprise databases, ensure that the service user has the necessary DB/File access rights).

Verifying the success of the recovery procedure

Check the historical log and run an import action to verify that the BigFix Compliance Application is successfully restored.

Procedure

Do the following steps to ensure that the BigFix Application Server is successfully restored.

1. Go to BigFix Compliance web interface and login with Administrator rights to verify that the log in works properly.
2. Go to **Management** > **Import** and verify the historical log shown in the page frame.

Appendix A. Example Reports

View examples of the various BigFix Compliance reports.

The following table lists examples of reports that you can generate in BigFix Compliance.

Table 11. Examples of BigFix Compliance reports

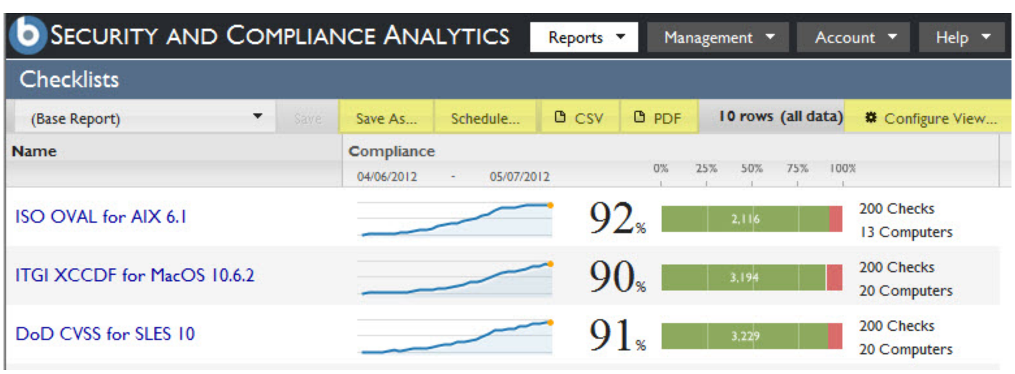
Name of Report	Location	Field or Graph Names	Other functions	Export Format
Checklist List	From the console, click **Reports** > **Checklists**	**Name**, **Compliance**	**Save As** and **Schedule**	.CSV and .PDF
Checklist Overview	From the console, click **Reports** > **Checklists**. Click any of the checklists that are displayed.	Compliance History, Computers by Compliance Quartile, Check Results History	**Save As**, **Schedule**, and **Configure View**.	.PDF
Checks List	From the console, click **Reports** > **Checks**	Name, Desired Values, Compliance	**Save As**, **Schedule**, and **Configure View**.	.CSV and .PDF,
Check Overview	From the console, click **Reports** > **Checks**	Compliance History, Check Results History, overall compliance percentage	**Save As**, **Schedule**, and **Configure View**.	.PDF
Computers List	From the console, click **Reports** > **Computers**	Computer Name, Last Seen, Vulnerability history, and Overall compliance	**Save As**, **Schedule**, and **Configure View**.	.CSV and PDF
Computer Overview	From the console, click **Reports** > **Overview**	Compliance history, Computers by Compliance Quartile, and Check results history	**Save As**, **Schedule**, and **Configure View**.	.PDF
Computer Groups List	From the console, click **Reports** > **Computer Groups**	Name, Children (subgroups), Vulnerability history, and Compliance in a list format	**Save As**, **Schedule**, and **Configure View**.	.CSV and .PDF

Table 11. Examples of BigFix Compliance reports (continued)

Name of Report	Location	Field or Graph Names	Other functions	Export Format
Computer Group Overview	From the console, click **Reports** > **Computer Groups**. Click any computer group in the list.	Compliance history, computers by compliance quartile, check results history, and vulnerability history	**Save As**, **Schedule**, and **Configure View**.	.PDF
Check Results List	From the console, click **Reports** > **Check Results**	Checklist, check name, computer name, the date results were last seen, and level of compliance	**Save As**, **Schedule**, and **Configure View**.	.CSV and .PDF
Vulnerabilities	From the console, click **Reports** > **Vulnerabilities** or **Reports** > **Vulnerability Results**	CVE ID and Vulnerability History	**Save As**, **Schedule**, and **Configure View**.	.CSV and .PDF

Checklist List Report

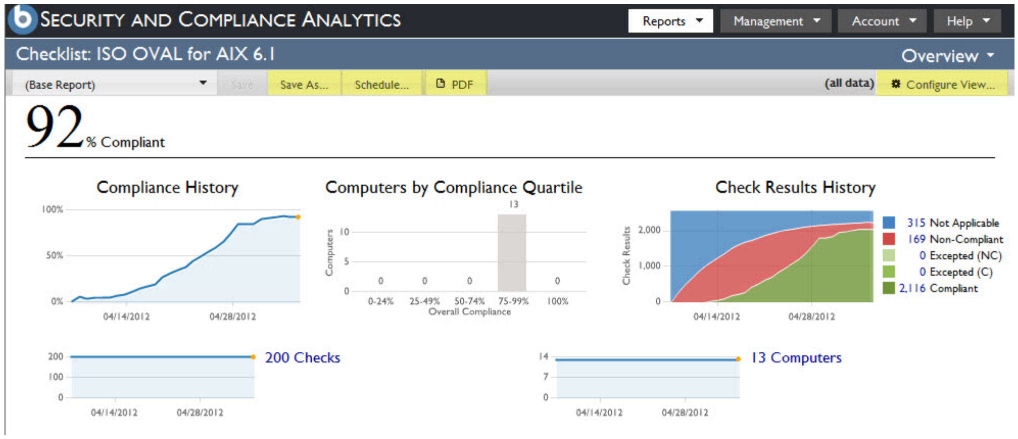
To access the Checklist List Report, click the Reports drop-down menu at the top of the console and select Checklists. This report displays data through name and compliance percentage fields. Use the links across the top to Save As, Schedule, export to .csv or .pdf, and Configure View.



Checklist Overview Report

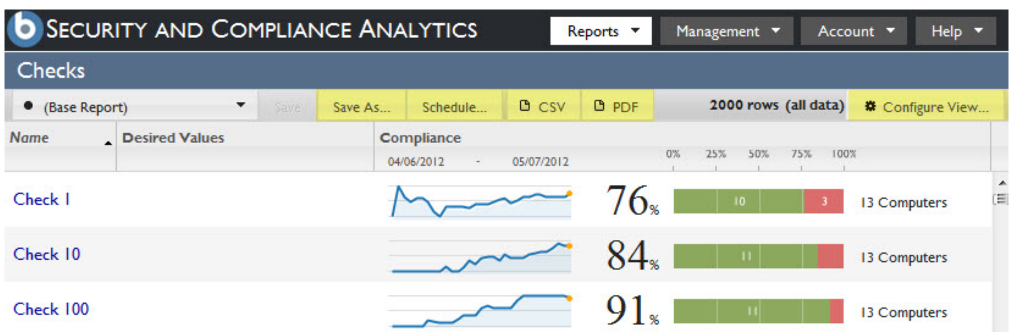
To access the Checklists Overview Report, click the Reports drop-down menu at the top of the console and select Checklists. The Checklist Overview Report is a drilldown of the Checklists List report. To access this view, click any checklist displayed. The Overview presents a graphic representation of compliance history, computers by compliance quartile, and check results history with an overall

compliance percentage shown in the top left corner of the console. Use the links across the top to Save As, Schedule, export to .pdf, and Configure View.



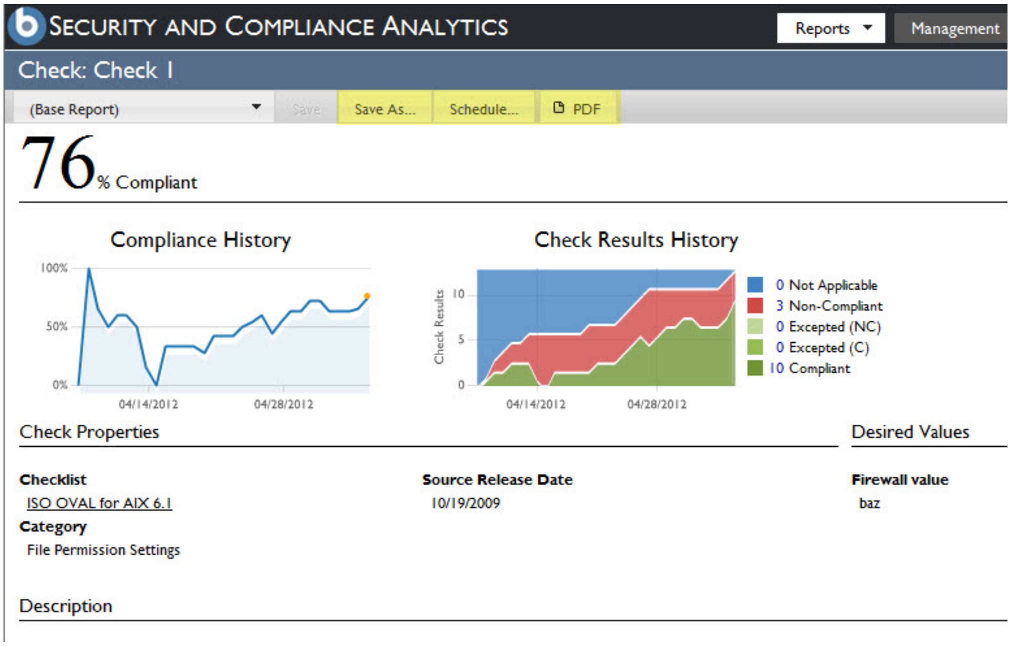
Checks List Report

To access the Checks List Report, click the Reports dropdown menu at the top of the console and select Checks. The Checks List report includes fields name, desired values, and compliance. Use the links across the top to Save As, Schedule, export to .csv and .pdf, and Configure View.



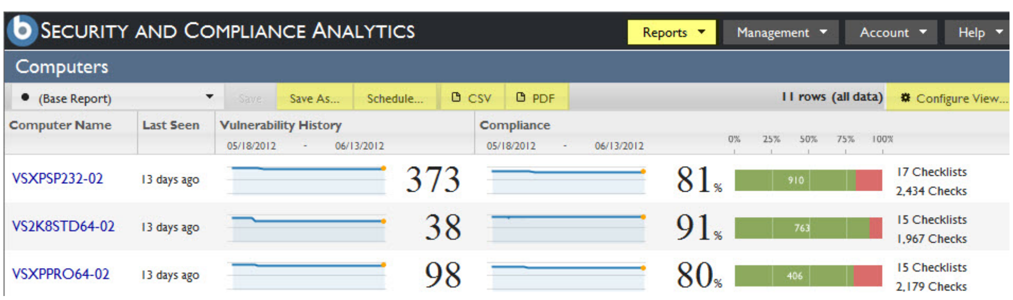
Check Overview Report

To access the Checks "Overview" Report, click the Reports dropdown menu at the top of the console and select Checks. This report is a drilldown of the Checks "List" report. To access this view, click any check in the list. The Checks Overview report presents a graphic representation of Compliance and Check Results history with an overall compliance percentage shown in the top left corner of the console. Use the links across the top to Save As, Schedule, export to .pdf, and Configure View.



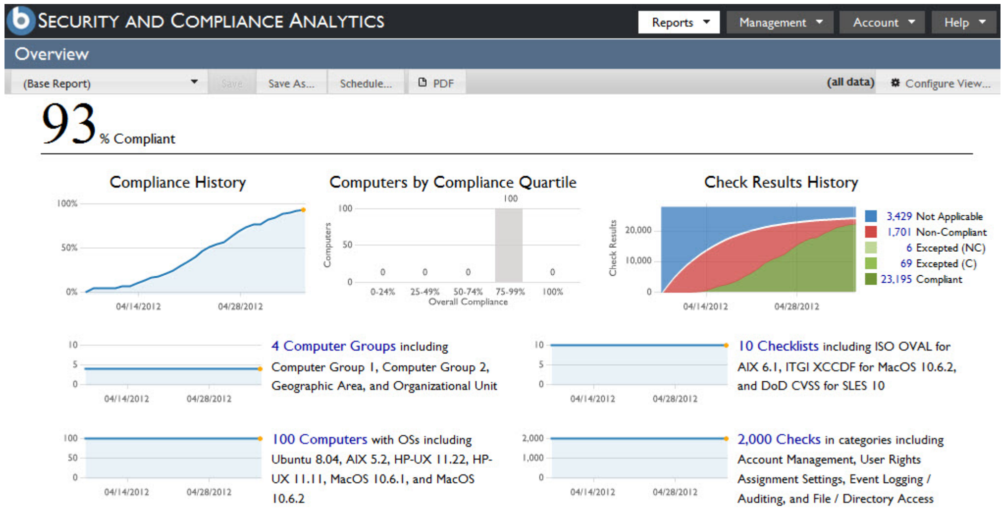
Computers List Report

To access the Computers List Report, click the Reports drop-down menu at the top of the console and select Computers. This report includes fields for computer name, last seen, vulnerability history, and overall compliance. Use the links across the top to Save As, Schedule, export to .csv or .pdf, and Configure View.



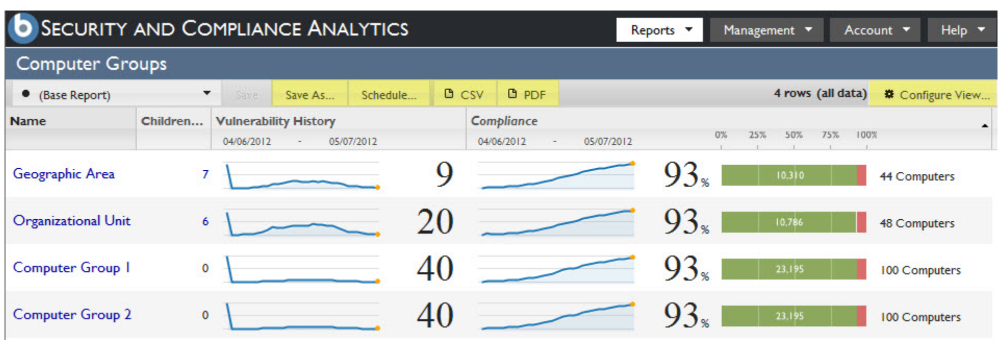
Computer Overview Report

To access the Computer Overview Report, click the Reports drop-down menu at the top of the console and select Overview. This report includes a graphic representation of your compliance history, check results history, and vulnerability. Use the links across the top to Save As, Schedule, export to .pdf, and Configure View.



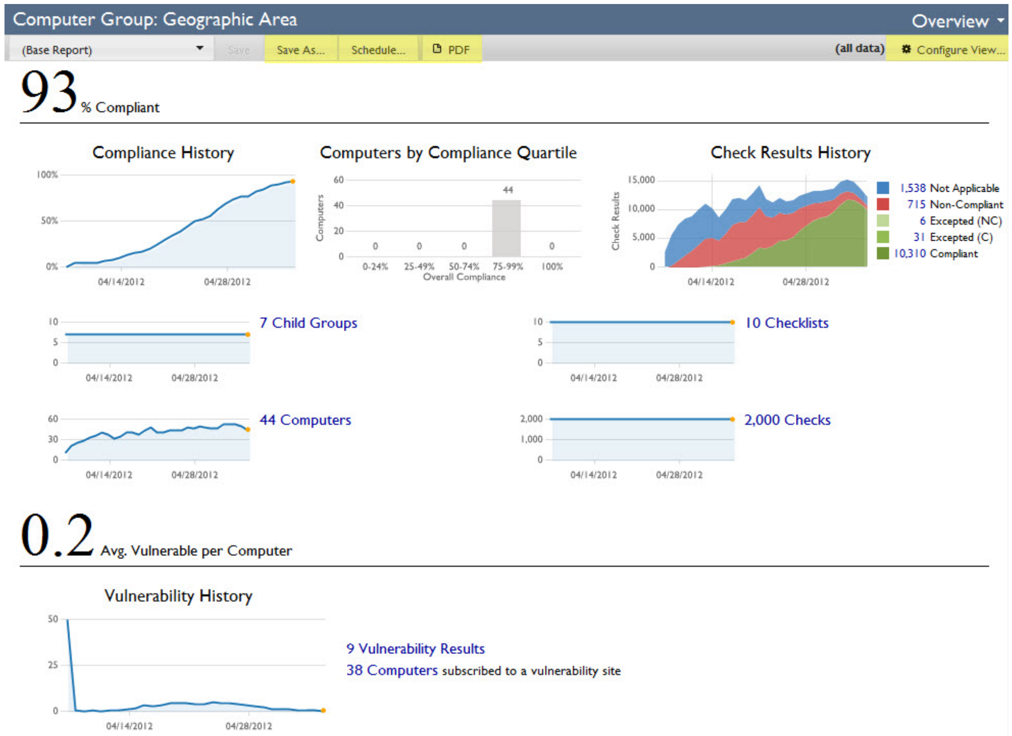
Computer Groups List Report

To access the Computer Groups List Report, click the Reports drop-down menu at the top of the console and select Computer Groups. This report includes fields for name, sub-groups (children), vulnerability history, and compliance in a list format. Use the links across the top to Save As, Schedule, Configure View, or to export the report as .csv or .pdf.



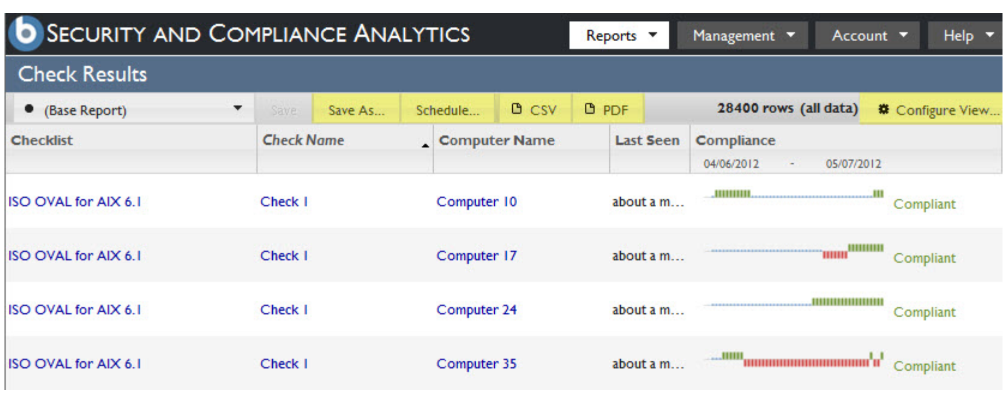
Computer Group Overview Report

To access the Computer Group Overview Report, click the Reports drop-down menu at the top of the console and select Computer Groups. This report is a drill down of the Computer Groups List Report, and can be accessed by clicking any computer group in the list on the initial screen. This graphic representation of computer groups shows compliance history, computers by compliance quartile, check results history, and vulnerability history. Use the links across the top to Save As, Schedule, export to .pdf, or Configure View.



Check Results List Report

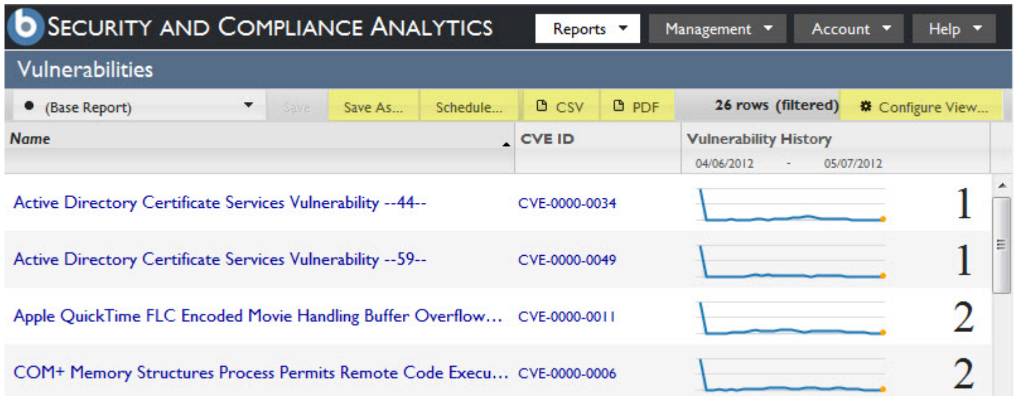
To access the Check Results List Report, click the Reports drop-down menu at the top of the console and select Check Results. This report includes fields for checklist, check name, computer name, the date results were last seen, and level of compliance. Use the links across the top to Save As, Schedule, Configure View, or to export the report as .csv or .pdf.



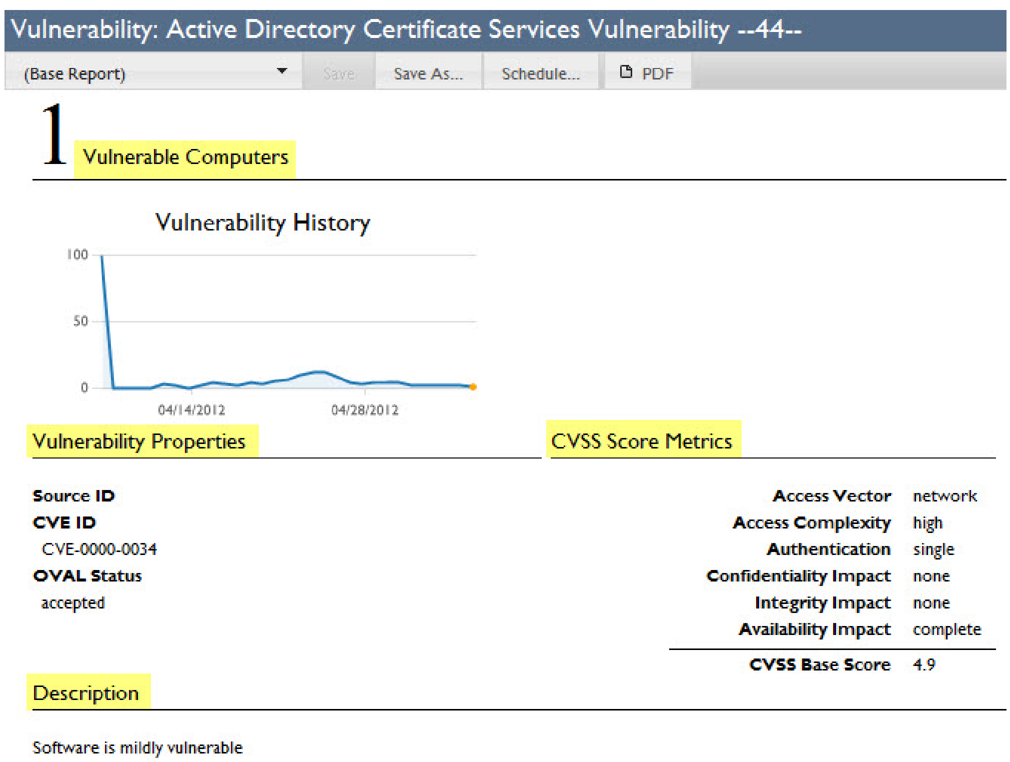
Vulnerabilities Report

To access the Vulnerabilities Report, click the Reports drop-down menu at the top of the console and select either Vulnerabilties or Vulnerability Results. The Vulnerabilities Report organizes data through name, CVE ID and Vulnerability History fields.

By default, the Vulnerabilities list shows vulnerability checks on your deployment to which at least one or more computers are vulnerable. To modify how the vulnerabilities in your deployment presents, click the Configure View button at the top fo the console and use the Filter submenu. Use the links across the top to Save As, Schedule, Configure View, or to export the report as .csv or .pdf.



To access the Vulnerability Overview report, click any name in the Vulnerabilities List report. This report presents a graphic representation of vulnerability history, as well as vulnerability properties, CVSS score metrics, and a description of the vulnerability.



Appendix B. Support

For more information about this product, see the following resources:

- IBM® Knowledge Center
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the “Web at Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Printed in USA